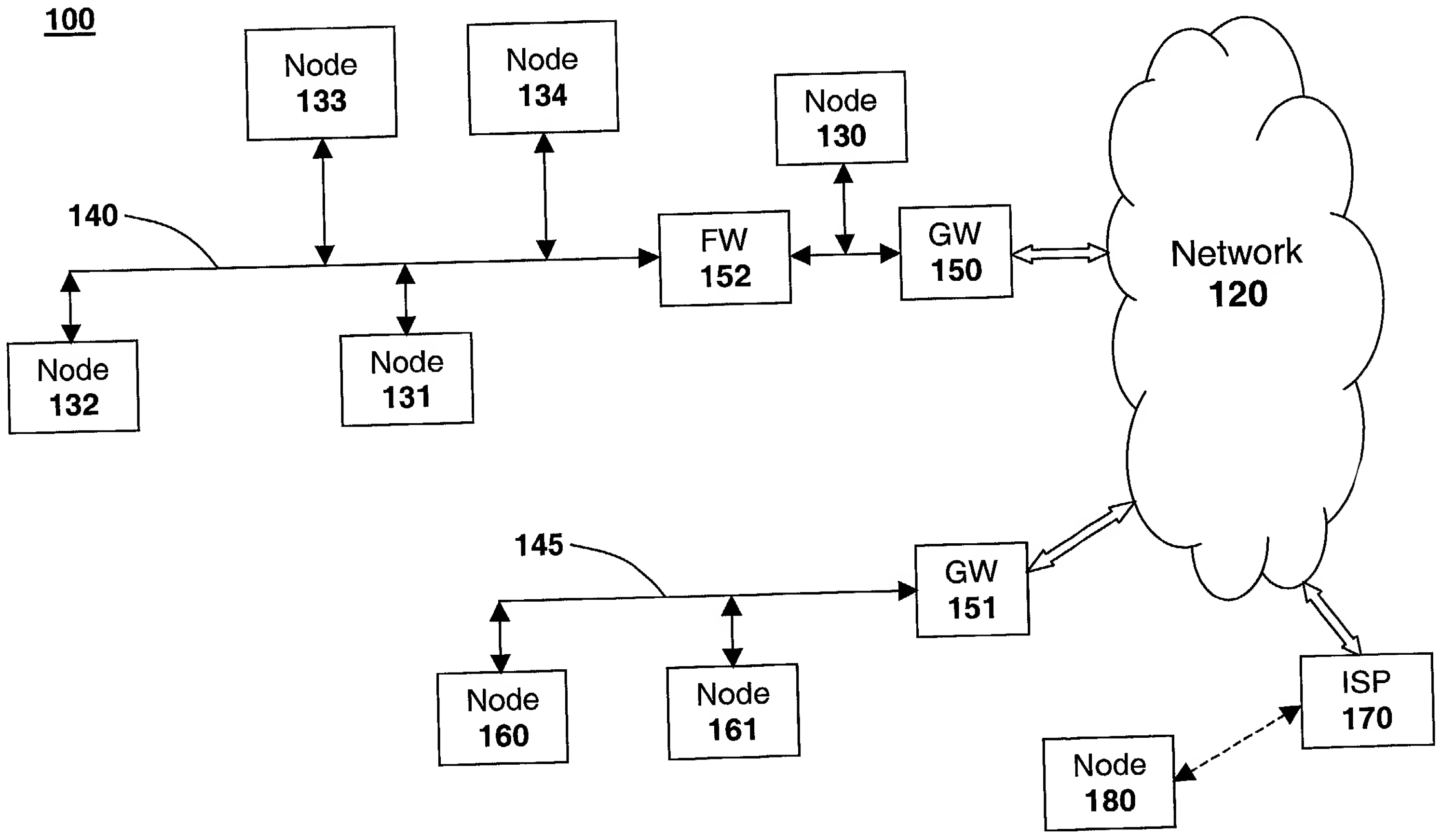
100
Node 133
Node 134
Node 130
140
FW 152
GW 150
Network 120
Node 132
Node 131
145
GW 151
Node 160
Node 161
ISP 170
Node 180

FIG. 1

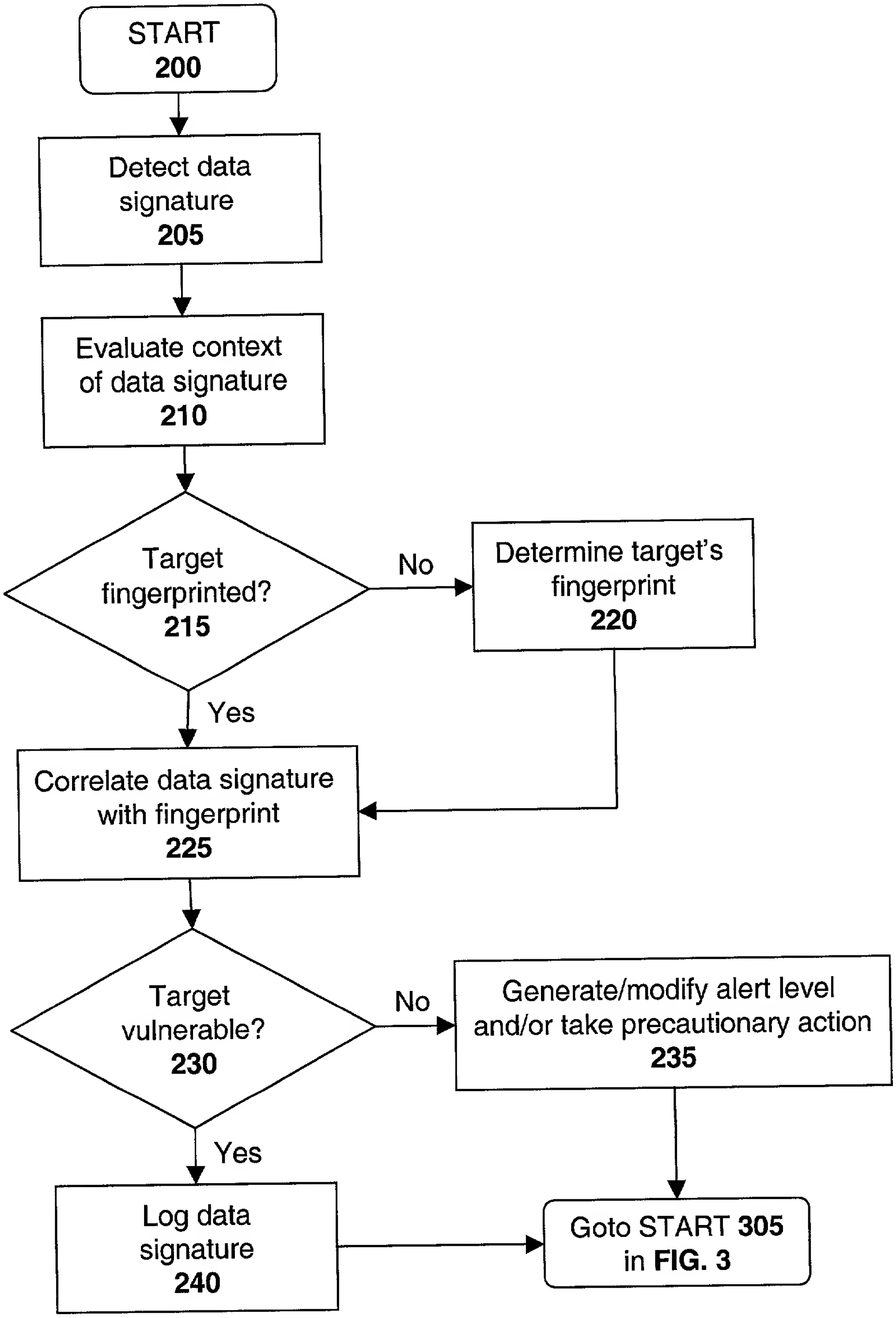
START
200
Detect data signature
205
Evaluate context of data signature
210
Target fingerprinted?
215
No
Determine target's fingerprint
220
Yes
Correlate data signature with fingerprint
225
Target vulnerable?
230
No
Generate/modify alert level and/or take precautionary action
235
Yes
Log data signature
240
Goto START 305 in FIG. 3

FIG. 2

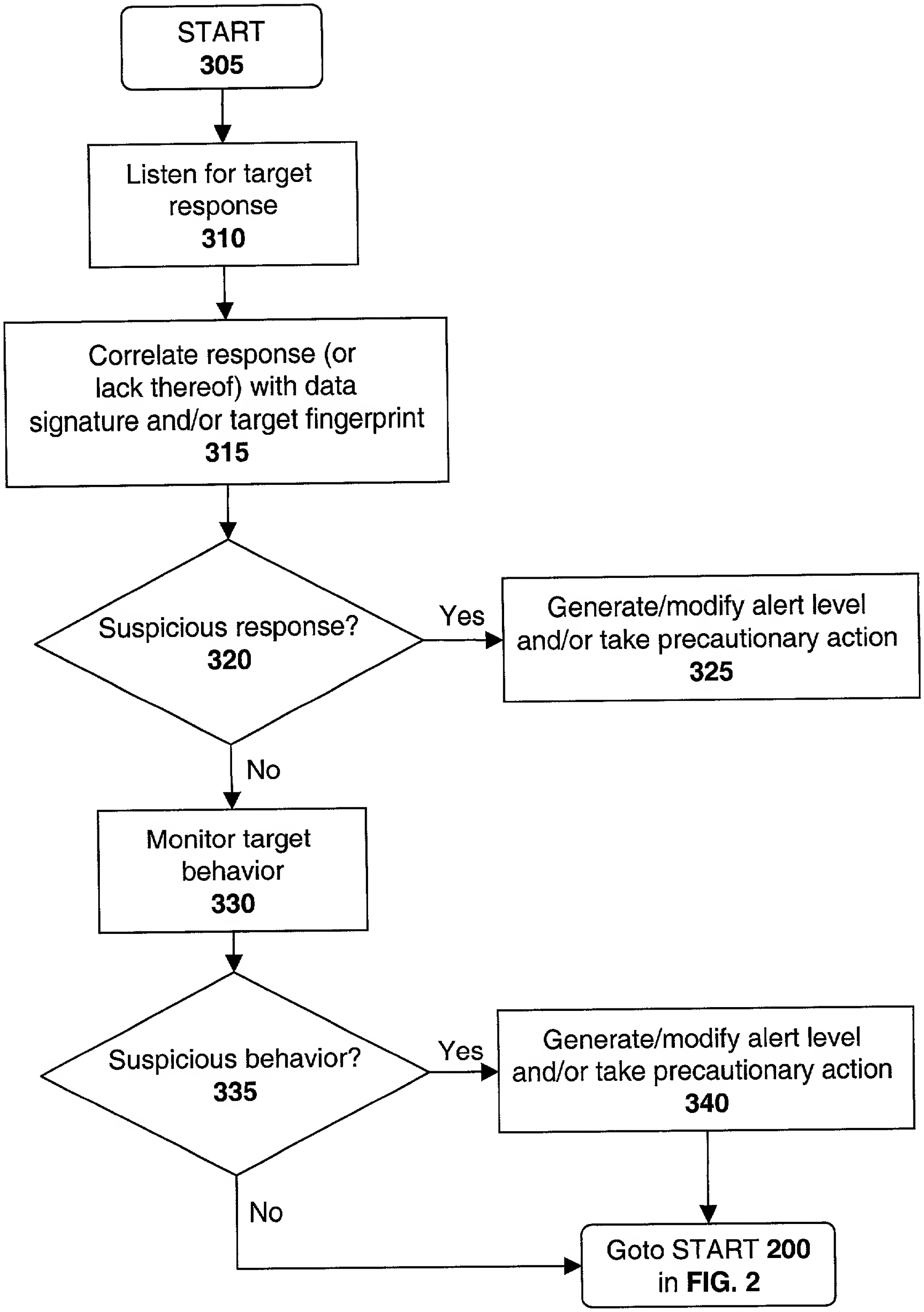
START
305
Listen for target response
310
Correlate response (or lack thereof) with data signature and/or target fingerprint
315
Suspicious response?
320
Yes
Generate/modify alert level and/or take precautionary action
325
No
Monitor target behavior
330
Suspicious behavior?
335
Yes
Generate/modify alert level and/or take precautionary action
340
No
Goto START 200 in FIG. 2

FIG. 3

Contextual Information for Data Signature Evaluation

Data Signature	Context	Severity/Alert Condition (0-5)
"/cgi-bin/phf"	HTTP URL	4
"/cgi-bin/phf"	Email header	0
"/cgi-bin/phf"	HTML HREF	3
".exe"	TFTP filename	2

FIG. 4

Exemplary Fingerprint Requests and Target Responses

FTP (file transfer):

```
220 rh5.robertgraham.com FTP server (version wu-2.4.2-academ [BETA-15] (1) Sat Nov 1
03:08:32 EST 1997) ready.
```

Telnet

```
Red Hat Linux release 5.0 (Hurricane)
kernel 2.0.31 on an i486
login:
```

SMTP (mail)

```
220 rh5.robertgraham.com ESMTP Sendmail 8.8.7/8.8.7; Mon, 29 Nov 1999  23:28:31-0800
```

Finger (user information)

```
Login Name     Tty   Idle  Login Time    office   office
Phone
rob  Robert David Graham p0 Nov 29 22:51      (gandalf)
root    root                      p1 Nov 29 23:34
(10.17.128.201:0.0)
```

HTTP

```
HTTP/1.0 200 OK
Date:  Tue, 30 Nov 1997 07:34:59  GMT
Server:  Apache/1.2.4
Last-Modified:  Thu, 06 Nov 1997 18:20:06 GMT
Accept-Ranges:  bytes
Content-Length:  1928
Content-Type:  text/html
```

HTTP

```
Date: Fri, 01 Jun 2001 20:38:03 GMT
Server: Apache/1.3.14 (Unix)  (Red-Hat/Linux) mod_ssl/2.7.1 OpenSSL/0.9.5a DAV/1.0.2
PHP/4.0.4pl1 mod_perl/1.24
Last-Modified: Wed, 18 Oct 2000 22:31:33 GMT
ETag: "9327c-b4a-39ee24c5"
Accept-Ranges: bytes
Content-Length: 2890
Connection: close
Content-Type: text/html
```

POP3

```
+OK  POP3  rh5.robertgraham.com  v4.39  server  ready
```

IMAP

```
* OK  rh5.robertgraham.com  IMAP4rev1  v10.190 server ready
```

SMB

```
SMB: ----- Setup Account AndX Header -----
SMB:
SMB: Word count          = 3
SMB: Parameter words     = 750080000000
SMB: Byte Count          = 87
SMB: Byte parameters     = 00570069006E006400....
SMB: AndX command        = 75 (Tree Connect AndX)
SMB: AndX reserved(MBZ) = 00
SMB: AndX offset         = 0080
SMB: Request Mode = 0000
SMB:  .... ....  .... ...0 = Not logged in as 'Guest'
SMB: Byte Count              = 87
SMB: Server's Native OS      = Windows NT 4.0
SMB: Server's Native LAN Man = NT LAN Manager 4.0
SMB: Server's Primary Domain = AMPHLETT
```

FIG. 5

Target Vulnerabilities

Target Fingerprint	Data Signature (may be context-based)	Severity/Alert Condition (0-5)
OS: Apache Ver >= 1.2 Processor: any BIOS: any	"/cgi-bin/phf" in HTTP Header	0
OS: Apache Ver < 1.2 Processor: any BIOS: any	"/cgi-bin/phf" in HTTP Header	4
OS: IIS Processor: any BIOS: any	"/cgi-bin/phf" in HTTP Header	0
OS: Netscape Enterprise Server Processor: any BIOS: any	"/cgi-bin/phf" in HTTP Header	0
OS: any Processor: Intel BIOS: any	09090909	3
OS: any Processor: Non-Intel BIOS: any	09090909	0

FIG. 6

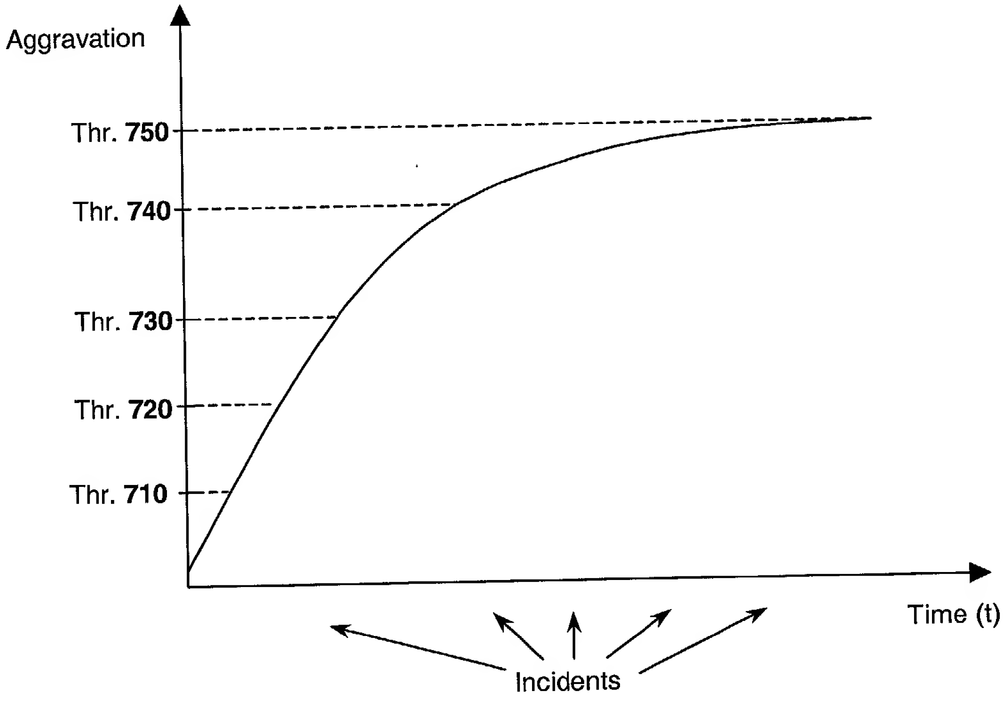
Aggravation
Thr. 750
Thr. 740
Thr. 730
Thr. 720
Thr. 710
Time (t)
Incidents

FIG. 7

```
 220 mandrake.intra.networkice.com FTP server (Version wu-
2.5.0(1) Sat May 22 11:15:07 GMT 1999) ready.

-> USER rob

   331 Password required for rob.

-> PASS Cerveza2

   230 User rob logged in.

-> SYS RETR /etc/passwd

   500 'SYS RETR /etc/passwd': command not understood.

-> PORT 10,10,0,135,4,1

   200 PORT command successful.

-> RETR /etc/passwd

   150 Opening ASCII mode data connection for /etc/passwd
(2661 bytes).

   226 Transfer complete.

-> RNFR /etc/passwd

   350 File exists, ready for destination name

-> RETR /tmp/etc/passwd

   550 /tmp/etc/passwd: No such file or directory.

-> QUIT

   221-You have transferred 2719 bytes in 1 files.

   221-Total traffic for this session was 3397 bytes in 1
transfers.

   221-Thank you for using the FTP service on
mandrake.intra.networkice.com.

   221 Goodbye.
```

FIG. 8

Excerpt from RFC 959

For each command or command sequence there are three possible outcomes: success (S), failure (F), and error (E). In the state diagrams below we use the symbol B for "begin", and the symbol W for "wait for reply".

```
                      1
+---+   USER    +---+------------->+---+
| B |---------->| W | 2       ---->| E |
+---+           +---+------  |  -->+---+
                 | |       | | |
               3 | | 4,5   | | |
   --------------   -----  | | |
  |                     |  | | |
  |                     |  | | |
  |                 ---------  |
  |               1|    |  |   |
  V                |    |  |   |
+---+   PASS    +---+ 2 |  ------->+---+
|   |---------->| W |------------->| S |
+---+           +---+   ---------->+---+
                 | |   | |     |
               3 | |4,5| |     |
   --------------   --------   |
  |                    | |  |  |
  |                    | |  |  |
  |                 -----------
  |             1,3|   | |  |
  V                |  2| |  |
+---+   ACCT    +---+--  |   ----->+---+
|   |---------->| W | 4,5 -------->| F |
+---+           +---+------------->+---+
```

FIG. 9

Snort 1.7 Signature

```
alert TCP $EXTERNAL any -> $INTERNAL 21 (
     msg: "IDS213/ftp_ftp-passwd-retrieval-retr";
     content: "RETR"; nocase;
     content: "passwd";)
```

Sample signature using one embodiment of the present system

```
alert TCP $EXTERNAL any -> $INTERNAL $FTP (
     msg: "IDS213/ftp_ftp-passwd-retrieval-retr";
     FTP.filename: "*/passwd";
     FTP.banner: "*Version wu-2*";
     FTP.response: "2??";
     FTP.response: "3??";
     )
```

FIG. 10

```
alert TCP $EXTERNAL any -> $INTERNAL $HTTP (
     msg: "system32/cmd.exe";
     HTTP.url: "*/system32/cmd.exe";
     HTTP.server: "IIS/*";
     +HTTP.response: "5??";
     -HTTP.response: "4??";
     -HTTP.response: "2??";
     )

alert TCP $EXTERNAL any -> $INTERNAL $HTTP (
     msg: "IIS malformed HTW";
     HTTP.url.extension: "*.htw";
     HTTP.server: "IIS/*";
     -HTTP.response: "5??";
     -HTTP.response: "4??";
     +HTTP.response: "2??";
     )
```

FIG. 11

```
RedHat 6.2
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100021    1   udp   1024  nlockmgr
    100021    3   udp   1024  nlockmgr
    100021    1   tcp   1024  nlockmgr
    100021    3   tcp   1024  nlockmgr
    100024    1   udp    980  status
    100024    1   tcp    982  status

RedHat 7.0
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100021    1   udp   1024  nlockmgr
    100021    3   udp   1024  nlockmgr
    100024    1   udp   1025  status
    100024    1   tcp   1024  status

Solaris 8
   program vers proto   port
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100232   10   udp  32772  sadmind
    100011    1   udp  32773  rquotad
    100002    2   udp  32774  rusersd
    100002    3   udp  32774  rusersd
    100002    2   tcp  32771  rusersd
    100002    3   tcp  32771  rusersd
    100012    1   udp  32775  sprayd
    100008    1   udp  32776  walld
    100001    2   udp  32777  rstatd
    100001    3   udp  32777  rstatd
    100001    4   udp  32777  rstatd
    100024    1   udp  32778  status
    100021    1   udp   4045  nlockmgr
    100021    2   udp   4045  nlockmgr
    100021    3   udp   4045  nlockmgr
    100021    4   udp   4045  nlockmgr
    100024    1   tcp  32772  status
    100133    1   udp  32778
    100133    1   tcp  32772
    100083    1   tcp  32773
    100221    1   tcp  32774
    100235    1   tcp  32775
    100021    1   tcp   4045  nlockmgr
    100021    2   tcp   4045  nlockmgr
    100021    3   tcp   4045  nlockmgr
    100021    4   tcp   4045  nlockmgr
    100068    2   udp  32779
    100068    3   udp  32779
    100068    4   udp  32779
    100068    5   udp  32779
    300326    4   tcp  32776
    300598    1   udp  32786
    300598    1   tcp  32778
 805306368    1   udp  32786
 805306368    1   tcp  32778
    100249    1   udp  32787
    100249    1   tcp  32779
1289637086    5   tcp  32803
1289637086    1   tcp  32803
```

FIG. 12